Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: 2/13/2019
2. Name of company(s) covered by this certification: Alta Municipal Utilities
3. Form 499 Filer ID: 820938
4. Name of signatory: Randy Tilk
5. Title of signatory: Utility Manager
6. Certification:

I, Randy Tilk, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.,* proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachments: Accompanying Statement explaining CPNI procedures

Alta Municipal Utilities
Form 499 Filer ID 820938
Accompanying Statement to Annual Certification of CPNI

Alta Municipal Utilities (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

The Board of Trustees of the Company, on November 7, 2007, adopted by Resolution an employee manual relating to the rules and disciplinary action in strict adherence of the CPNI rules as defined by the FCC.

Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training:

All Company personnel received training in November of 2007 that included a complete review of the CPNI Employee Manual. The rules will be reviewed with employees on an annual basis or as needed. Any new employee will be trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI.

Employees are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

Customer Notification and Request for Approval to Use CPNI

The Company has provided notification to its customers of their CPNI rights and has asked for the customer's approval to use CPNI via the opt-out method.

The status of a customer's CPNI approval is prominently displayed as soon as the customer's account is accessed so that employees can readily identify customers that have restricted the use of their CPNI.

The Company does not share CPNI with any joint venture partners, independent contractors or any third party.

For the customers that have opted-out and said the Company cannot use their CPNI, that decision will remain valid until the customer changes it.

The company sends the opt-out notice every two years to those customers that have not previously opted out.

The Company will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

Marketing Campaigns

The Company has not used CPNI for any sales or marketing campaign. If the Company decides to use CPNI for any marketing campaign, both management and the Compliance Officer will review it to ensure that it is in compliance with the rules.

Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

In-office visit - the customer must provide a valid photo ID matching the customer's account information.

Customer-initiated call where password has been established – the customer must provide his/her pre-established password and must be listed as a contact on the account.

Customer-initiated call where password has not been established – the customer is authenticated by providing an answer to a pre-established question and must be listed as a contact on the account.

Call detail information – if the customer wants to discuss call detail information, the following guidelines are followed:

- If the customer has established a password and provides it without any prompt from the Company, the call detail information will be provided to the customer.
- If the customer has not established a password or cannot remember the password but has been authenticated by another means:
    - If the customer can provide all of the call detail information (telephone number called, when it was called, and the amount of the call) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.
    - If the customer cannot provide all of the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

Notification of Account Changes

The Company promptly notifies customers whenever a change is made to any of the following:

- Password.
- Customer response to a back-up means of authentication for a password
- Address of record.

The notification to the customer will be made either by a Company-originated voicemail or text message to the telephone number of record or sent to the address (postal or electronic) of record.

The Company has a process for tracking when a notification is required and for recording when and how the notification is made.

Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at http://www.fcc.gov/eb/cpni.

- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.

- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.

- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

- Include a summary of the breach in the annual compliance certificate filed with the FCC.

Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

Record Retention

The Company retains all information regarding CPNI. Following is the minimum retention period we have established for specific items:

- CPNI notification and records of approval – one year
- Marketing campaigns – one year
- Breaches – two years
- Annual certification – five years
- Employee training certification – two years
- All other information – two years